I claim:

1. A method of generating a password for at least one application using a single key, said method comprising the steps of:

receiving said single key;

receiving a first application name associated with a first application; and

generating a first password for said first application, based on at least said single key and said first application name.

2. The method according to claim 1, comprising the further steps of:

receiving a second application name associated with a second application; and

generating a second password for said second application, based on said single key and said second application name.

3. The method according to claim 1, comprising the further step of:

receiving a time period;

wherein generating said first password is further based on said time period.

4. The method according to claim 1, comprising the further step of:

receiving first password constraints for said first password;

wherein generating said first password is further based on said first password constraints.

5. The method according to claim 1, wherein generating said first password utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

6. The method according to claim 1, comprising the further step of:

generating a first userid for said first application, based on at least said single key and said first application name.

7. The method according to claim 6, comprising the further step of:

receiving a first userid time period;

wherein generating said first userid is further based on said first userid time period.

8. The method according to claim 6, comprising the further step of:

receiving first userid constraints for said first userid;

wherein generating said first password is further based on said first userid constraints.

9. The method according to claim 6, wherein generating said first userid utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

10. The method according to claim 1, wherein said first application is selected from the group of applications consisting of bank account, Internet email account, Internet website, and computer account.

11. A method of generating a password for a plurality of applications using a single key, said method comprising the steps of:

receiving a single key;

receiving a first application name associated with a first application;

generating a first password for said first application, based on at least said single key and said first application name;

receiving a second application name associated with a second application; and

generating a second password for said second application, based on at least said single key and said second application name.

12. The method according to claim 11, comprising the further step of:

receiving first password constraints for said first application;

wherein generating said first password is further based on said first password constraints.

13. The method according to claim 11, comprising the further step of:

generating a first userid for said first application based on at least said single key and said first application name.

14. The method according to claim 13, comprising the further step of:

receiving first userid constraints for said first application;

wherein generating said first userid is further based on said first userid constraints.

15. The method according to claim 11, comprising the further step of:

receiving second password constraints for said second application;

wherein generating said second password is further based on said second password constraints.

16. The method according to claim 11, comprising the further step of:

generating a second userid for said second application based on at least said single key and said second application name.

17. The method according to claim 16, comprising the further step of:

receiving second userid constraints for said second application;

wherein generating said second userid is further based on said second userid constraints.

18. An apparatus for generating a password for at least one application using a single key, said apparatus comprising:

means for receiving said single key;

means for receiving a first application name associated with a first application; and

means for generating a first password for said first application, based on at least said single key and said first application name.

19. The apparatus according to claim 18, further comprising:

means for receiving a second application name associated with a second application; and

means for generating a second password for said second application, based on said single key and said second application name.

20. The apparatus according to claim 18, further comprising:

means for receiving a time period;

wherein said means for generating said first password utilises said time period.

21. The apparatus according to claim 18, further comprising:

means for receiving first password constraints for said first password;

wherein said means for generating said first password utilises said first password constraints.

22. The apparatus according to claim 18, wherein said means for generating said first password utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

23. The apparatus according to claim 18, further comprising:

means for generating a first userid for said first application, based on at least said single key and said first application name.

24. The apparatus according to claim 23, further comprising:

means for receiving a first userid time period;

wherein said means for generating said first userid utilises said first userid time period.

25. The apparatus according to claim 23, further comprising:

means for receiving first userid constraints for said first userid;

wherein said means for generating said first password utilises said first userid constraints.

26. The apparatus according to claim 23, wherein said means for generating said first userid utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

27. A computer program product comprising a computer readable medium having a computer program recorded therein for generating a password for at least one application using a single key, said computer program comprising:

computer program code means for receiving said single key;

computer program code means for receiving a first application name associated with a first application; and

computer program code means for generating a first password for said first application, based on at least said single key and said first application name.

28. The computer program product according to claim 27, further comprising:

computer program code means for receiving a second application name associated with a second application; and

computer program code means for generating a second password for said second application, based on said single key and said second application name.

29 The computer program product according to claim 27, further comprising:

computer program code means for receiving a time period;

wherein said computer program code means for generating said first password utilises said time period.

30. The computer program product according to claim 27, further comprising:

computer program code means for receiving first password constraints for said first password;

wherein said computer program code means for generating said first password utilises said first password constraints.

31. The computer program product according to claim 27, wherein said computer program code means for generating said first password utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition,

International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

32. The computer program product according to claim 27, further comprising:

computer program code means for generating a first userid for said first application, based on at least said single key and said first application name.

33. The computer program product according to claim 32, further comprising:

computer program code means for receiving a first userid time period;

wherein said computer program code means for generating said first userid utilises said first userid time period.

34. The computer program product according to claim 32, further comprising:

computer program code means for receiving first userid constraints for said first userid;

wherein said computer program code means for generating said first password utilises said first userid constraints.

35. The computer program product according to claim 32, wherein said computer program code means for generating said first userid utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.